APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,370	07/31/2003	Stuart S. Kreitzer	CE11296JEM	2130

24273   7590   04/24/2009
MOTOROLA, INC
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER
PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 January 2009_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-7, 9-12 and 14-21_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-7, 9-12 and 14-21_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 1/16/2009 has been entered. Applicant has amended claims 1, 11, 14, and 21. Currently claims 1-7, 9-12, and 14-21 are pending in this application.

Response to Arguments

1.   Applicant's arguments filed 1/16/2009 have been fully considered but they are not persuasive for the following reason:

- Regarding **claim 1**, applicant argues that, "Independent claim 1 has been amended to clarify that following the switch, the symmetric traffic key established for the first mode of communication is shared between the multi-mode portable communication device and the second multi-mode portable communication device for the second mode of communication. Applicant respectfully submits that Wellig does not teach such a feature. In arguing that Wellig reads on this limitation, the Examiner refers to col. 12, lines 59-63 of that reference (see page 4 of the Office Action of July 18, 2008). That passage, however, merely explains that the mobile terminals may employ an encryption key for maintaining a secure data transmission when the mobile terminals are in a direct mode of communication. Wellig never mentions anything about re-using an encryption key that was established in any other form of communication prior to the direct mode of communciation."

- First of all examiner would like to point out that applicant admitted that the mobile terminals may employ an encryption key for maintaining a secure data transmission when the mobile terminals are in a direct mode of communication. Applicant argument that Wellig never mentions anything about re-using an encryption key that was established in any other form of communication prior to the direct mode of communciation is not found persuasive because Col 12, line 59-63 clearly discloses "However, **before any information is transmitted in DM**, the **two MTs have to agree on** further points such as the base modulation scheme or **an encryption key** for maintaining a secured data transmission. **This information exchange will be controlled by the AP by granted slot(s)**." This recitation clearly discloses that the encryption key that is used in DM is exchanged under the control by the AP thus the encryption key used in DM is derived in a non-direct mode because this part clearly requires two MTs to agree on an encryption key **before** any information is transmitted in DM. Therefore, Examiner maintain that Wellig still discloses "following the switch, the symmetric traffic key established for the first mode of communication is shared between the multi-mode portable communication device and the second multi-mode portable communication device for the second mode of communication". The rejection is maintained.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

Claims 14-21 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a processing unit is merely recited in independent claims 14 to be "operable to" establish a symmetric traffic key…, establish a secure communication session… and switch to at least…communication network and in claim 21 to be "operable to" store information…, establish a symmetric traffic key…, establish a secure communication session… and switch to at least...communication network. Thus, it is merely capable of performing the recited or desired functions as recited in the claims 14 and 21. In other words, there is no present tense, positively recited performing all these functions as recited in the claims 14 and 21. Thus, since the functions are not actually performed, they cannot be used operate a portable communication device in multiple modes as recited in claims 14 and 21. This situation clearly renders the entire subject matter of independent claims 14 and 21 and its respective dependent claims 15-20 indefinite within the second paragraph of 35 U.S.C. § 112.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed
> publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

<u>Claims 1, 5, 6, 9, 14, 17 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Wellig et al. (US 6,580,704 B1), hereinafter "Wellig".</u>

Regarding **Claims 1 and 14**, Wellig discloses a method and a portable communication device capable of operating in multiple modes, comprising:

establishing a symmetric traffic key between the multi-mode portable communication device (see, Fig. 1, Numeral 12) and a second multi-mode portable communication device (Fig. 1, Numeral 13) in a first mode of communication in a first communication network that supports a first communication protocol (see Fig. 1, Non-Direct Mode communication that includes AP for communication and also see, Column 12, 59-63);

switching to at least a second mode of communication in a different communication network that supports a different communication protocol (see, Fig. 1, "Direct Mode"); and

following the switch, sharing the symmetric traffic key established for the first mode of communication between the multi-mode portable communication device and the second multi-mode portable communication device for the second mode of

communication (see, Column 12, lines 59-63, for detailed explanation please refer to "response to argument" section above);

wherein the multi-mode device and the second multi-mode device communicate with one another using the first communication protocol over the first communication network (Fig. 1, Non-Direct mode) and using the different communication protocol over the different communication network (Fig. 1, Direct Mode).

Regarding **Claims 5 and 17**, the rejection of claims 1 and 14 is incorporated and Wellig further discloses wherein the step of switching to the second mode from the first mode comprises switching among modes comprising interconnect voice, dispatch voice, peer-to peer data, and peer-to-peer voice (see, Fig. 1, Direct mode is interpreted as a peer-to peer mode).

Regarding **Claim 6**, the rejection of claim 1 incorporated and Wellig further discloses wherein the step of switching to the second mode from the first mode comprises switching among communication protocols comprising CDMA, TDMA, GSM, and WLAN (see, Column 7, lines 2-4).

Regarding **Claims 9 and 19**, the rejection of claims 1 and 14 is incorporated and Wellig further discloses wherein the step of establishing a new communication session between the multi-mode portable communication device and the second portable communication device without requiring an APK key establishment process (see, Column 12, lines 59-63, MTs uses encryption key is negotiated during a Non-Direct mode and during direct mode, communication between 2 MTs is encrypted using that key).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 3 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Wellig in view of Schneier (Schneier, Applied Cryptography, Wiley, 2nd Edition,

Page 48), hereinafter, "Schneier".

Regarding **Claims 2 and 15**, Although Wellig discloses negotiating encryption to

be used in direct mode, during non-direct mode; Wellig does not expressly disclose a

system that uses Automatic Public Key Exchange techniques.

Schneier teaches using the public key exchange system using private keys along

with a public key of a peer unit before commencing secure communications (page 48).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use the public and private keys to perform the key exchange

as in Schneier in the system of Wellig. One of ordinary skill in the art would have been

motivated to do this because it would make key-exchange easier.

Regarding **Claim 3**, Although Wellig discloses negotiating encryption to be used

in direct mode, during non-direct mode; Wellig does not expressly disclose a system

that uses Automatic Public Key Exchange is implemented using public-key algorithms

such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

Schneier discloses a system that uses public-key algorithms for Public Key

Exchange techniques (page 48 paragraph 2).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use the public and private keys to perform the key exchange

as in Schneier in the system of Wellig. One of ordinary skill in the art would have been

motivated to do this because it would make key-exchange easier.

Claims 7 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Wellig in view of Whelan et al (6,965,674 B2), hereinafter, "Whelan".

Regarding **Claims 7 and 18**, the rejection of claims 1 and 14 is incorporated and

Wellig does not disclose the step of storing the symmetric traffic key in a phonebook

record associated with the second portable communication device or the traffic key is

stored in a recent call list that reflects recent communication between the portable

communication device and a second portable communication device.

Whelan discloses a system wherein the traffic key is stored in a recent call list

that reflects recent communication between the portable communication device and a

second portable communication device (column 5 lines 30-33; column 10 lines 19-42;

Fig. 4)

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to store the traffic key in a recent call list as in the system of

Whelan in the system of Wellig. One of ordinary skill in the art would have been

motivated to do this because it would make it impractical for a hacker to gather sufficient

network traffic using any one WEP key to decrypt that key (Whelan column 7 lines 54-65).

Claims 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wellig in view of Suzuki (5,390,252), hereinafter, "Suzuki".

Regarding **Claims 10 and 20**, the rejection of claim 1 is incorporated and Wellig discloses establishing encryption key during the first mode of communication. However, Wellig does not explicitly discloses establishing a symmetric traffic key between a first multi-mode portable communication device and the predetermined number of other multi-mode portable communication devices during an idle mode of the first multi-mode portable communication device.

Suzuki discloses establishing a symmetric traffic key between a first portable communication device and the predetermined number of other portable communication devices during an idle mode of the first portable communication device (column 5 line 60 to column 6 line 12, Note: the idle mode corresponds to the mode 1 because at this mode no information is being transferred, but the system is ready therefore making this an idle mode).

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to, establish encryption key between the first multi mode portable communication device and the second portable communication device in the system of Wellig, during an idle mode of the first multi-mode portable communication device as taught by Suzuki so that encryption key can be ready prior to

start of the non-direct mode of Wellig which would then reduce the time of the first mode

(non-Direct mode) of Wellig's system thus improving overall performance of the

system).

        Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Wellig in view of Schneier and further in view of the article by L-3 Communications,

hereinafter "L-3".

        Regarding **Claims 4 and 16**, Although Wellig discloses negotiating encryption to

be used in direct mode, during non-direct mode; Wellig does not expressly disclose a

system wherein the Automatic Public Key exchange is implemented by combining

public-key algorithms with a signaling scheme such as Future Narrow Band Digital

Terminal protocol.

        L-3 discloses a terminal that implements the Future Narrow Digital standard and

therefore protocol. The protocol includes key management and therefore key exchange

(page 1).

        At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use the future narrow band with digital terminal protocol as

disclosed by L-3 in the combined system of Wellig and Schneier. One of ordinary skill

in the art would have been motivated to do this because Future Narrow Band Digital

Terminal Protocol does not tie one down to a specific network, but instead assures

operation over a variety of narrow band wide band (L-3 page 1).

Claims 11 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Wellig in view of Suzuki and further in view of Schneier.

Regarding **Claims 11 and 21**, Wellig et al. (US 6,580704 B1) discloses a method

and system of establishing secure communications among a plurality of portable

communication devices, comprising the steps of:

storing information associated with a predetermined number of other portable

communication devices (see, Fig. 2);

establishing a secure communication session in a first mode of communication in

a first communication network that supports a first communication protocol between the

first multi-mode portable communication and at least one among the predetermined

number of other multi-mode portable communication devices (see Fig. 1, MT1 and MT2

in the mode of connection are connected to each other using access point)

switching to at least a second mode of communication in a second

communication network that is different from the first communication network and that

supports a second communication protocol that is different from the first communication

protocol (see, Fig. 1, "Direct Mode"); and

following the switch, sharing the same symmetric traffic key established for the

first mode of communication between the first multi-mode portable communication

device and the at least one among the predetermined number of other multi-mode

portable communication devices in the second mode of communication;

wherein the first multi-mode device and the other multi-mode device

communicate with one another using the first communication protocol over the first

communication network and using the second communication protocol over the second

communication network.

Wellig discloses establishing encryption key during the first mode of

communication. However, Wellig does not explicitly discloses establishing a symmetric

traffic key between a first multi-mode portable communication device and the

predetermined number of other multi-mode portable communication devices during an

idle mode of the first multi-mode portable communication device.

Suzuki discloses establishing a symmetric traffic key between a first portable

communication device and the predetermined number of other portable communication

devices during an idle mode of the first portable communication device (column 5 line

60 to column 6 line 12, Note: the idle mode corresponds to the mode 1 because at this

mode no information is being transferred, but the system is ready therefore making this

an idle mode).

Therefore, at the time the invention was made, it would have been obvious to a

person of ordinary skill in the art to, establish encryption key between the first multi

mode portable communication device and the second portable communication device in

the system of Wellig, during an idle mode of the first multi-mode portable

communication device as taught by Suzuki so that encryption key can be ready prior to

start of the non-direct mode of Wellig which would then reduce the time of the first mode

(non-Direct mode) of Wellig's system thus improving overall performance of the

system).

Although Wellig and Suzuki discloses encryption key establishment step, they do

not explicitly disclose that encryption key is established using an APK key establishment process.

Schneier discloses a system that uses public-key algorithms for Public Key Exchange techniques (page 48 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the public and private keys to perform the key exchange as in Schneier in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because it would make key-exchange easier.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wellig in view of Suzuki and Schneier and further in view of Howard, Jr. et al. (US 6,212,280 B1), hereinafter "Howard".

Regarding **Claim 12**, the rejection of claim 11 is incorporated and the combination of Wellig, Suzuki and Schneier as applied in the rejection of claim 11 does not explicitly discloses a system wherein the step of establishing a symmetric traffic key comprises contacting the predetermined number of other portable communication devices to determine if their respective keys have expired and performing a background exchange to re-establish a fresh key if the respective key has expired.

However, Howard discloses a system wherein the step of establishing a symmetric traffic key comprises contacting the predetermined number of other portable communication devices to determine if their respective keys have expired and performing a background exchange to re-establish a fresh key if the respective key has expired (see, Column 21, line 58 through Column 22 line 2).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to re-establish keys, in the combined system of Wellig, Suzuki and Schneier, when the traffic keys expires as taught by Howard so that clients can always have the latest key available to establish secure connections.

Conclusion

5.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435